IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CR. NO. 2:06cr214-MEF-WC**
	)	
DANIEL L. PLATT	)	

UNITED STATES'S RESPONSE TO DEFENDANT'S SUPPLEMENTAL MOTION TO SUPPRESS

Comes now the United States of America by and through Leura G. Canary, United States Attorney for the Middle District of Alabama and submits that Daniel L. Platt's ("Platt") motion to suppress and supplemental motion to suppress should be denied. Platt complains "that law enforcement in seizing and searching his computer exceeded the authority granted in the search warrant." (Doc. 36, para. 2). The defendant's complaint is meritless based upon the search warrant issued and the complete description outlined in Attachment A, of the items to be searched. In support of its position, the government submits this response:

1. The government re-alleges its entire argument and legal support submitted in Document 26-1, filed October 21, 2006. In addition, the government submits that the defendant's supplement to his motion should be summarily dismissed since the supplemental motion is only supported by conclusory assertions that do not take into consideration the search warrant in its entirety with the inclusion of Attachment A.

2. Attachment A, paragraph 13, states the following:

> 13. Any and all items described in paragraphs 1 - 12 above that are stored in the form of magnetic or electronic coding on computer media, or media capable of being read by a computer, with the aid of computer related equipment, including floppy diskettes, CD-ROMS, CD-Rs, CD-RWs, DVDs, fixed hard drives or removable hard disk[s] cartridges, software or memory in any form. The search procedure for electronic data contained

in computer operating software or memory devices, where performed on site or in a laboratory, or other controlled environment, may include the following techniques:

a. The seizure of any computer or computer related equipment or data, including floppy diskettes, CD-ROMS, CD-Rs, CD-RWs, DVDs, fixed hard drives or removable hard disk[s] cartridges, software or memory in any form containing material described above, and the removal thereof from the PREMISES for analysis by authorized personnel;

b. Surveying various file "directories" and the individual files they contain (analogous to looking [at] the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

c. "Opening" or cursorily reading the first few pages of such files in order to determine their precise contents;

d. "Scanning" storage areas to discover and possibly recover recently deleted data;

e. "Scanning storage areas for deliberately hidden files; or

f. Performing keyword searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation. Keywords include words relating to pornography, sex, genitalia, intercourse and topics relating to teen and pre-teen activities.

3. Defendant's motion does not take other pertinent parts of Attachment A, such as item 1, which clearly states that the property to be seized includes, "...commercial software and hardware, computer disks, ...system disk operating systems, ...hard drive and other computer related equipment... that may be used to depict child pornography..." Throughout Attachment A, reference is made to virtually any and everything that may contain depictions of child pornography. Attachment A should be taken as a whole, and should not be isolated to paragraph 13d. A reading of 13e, defeats defendant's argument, since 13e states that agents may search by "scanning storage areas for deliberately hidden files; or..." A deleted file can amount to a hidden

file, if the user has the software to retrieve the file as desired. Expert testimony has been presented in similar cases wherein a defendant has been convicted for possession of child pornography based upon images located as deleted images.

II. Forensic Argument

Two Tenth Circuit cases have addressed the sufficiency of the evidence to find an individual guilty of knowingly possessing child pornography under § 2252A(a)(95)(B) for viewing such images over the Internet.

In United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002), the defendant had been previously convicted of sexually abusing a child. Tucker was on parole and under supervision of the Adult Probation and Parole office. As part of Tucker's supervision, Tucker was forbidden from "view[ing] or hav[ing] in [his] possession any material exploiting children or depicting unconsensual sex acts or acts involving force or violence." Tucker at 1195. During a search by his residence, parole officers located a computer, which was also searched. Some 27,000 images were stored on Tucker's computer, of which approximately ninety to ninety-five percent were child pornography. Id. at 1197. Some of the images were "thumbnails" and others were larger. The images were recovered from the Web browsers' cache files, the computer "unallocated" hard drive space, and the computer recycle bin.

Tucker argued, unsuccessfully, that the Web browser automatically cached image files without his input, and he did not voluntarily possess the images. Id. The district court disagreed. The court held that,

> "Tucker possessed child pornography under the meaning of §2252A(a)(5)(B) because he had control over the images cached on this hard drive....The court reasoned that Tucker's habit of

> manually deleting images from the cache files established that he exercised control over them....The district court also rejected Tucker's argument that since the Web browser automatically cached image files without his input, he did not voluntarily possess the images. The district court reasoned that Tucker visited Web sites for the purpose of viewing child pornography, and that '[t]he images would not have been saved to his cache file had Tucker not volitionally reached out for them.' (citations omitted) Finally, the district court concluded that Tucker's possession was knowing, since he purposefully visited Web sites containing child pornography knowing that the images would be stored on his computer's hard drive."

Tucker, at 1198.

The Tenth Circuit chose not to offer an opinion on two questions: (1) whether the mere viewing of child pornography on the Internet, absent caching or otherwise saving the image, would meet the statutory definition of possession; and (2) whether an individual could be found guilty of knowingly possessing child pornography if he viewed such images over the Internet but was ignorant of the fact that his Web browser cached such images. Almost three years later, the Tenth Circuit answered the second question.

In United States v. Bass, 411 F.3d 1198, the defendant was identified from an FBI initiative called "Operation Candyman." "Candyman" was a "free Internet service that enabled interested people to collect and distribute child pornography and sexually explicit images of children." Bass, at 1200 (quoting, United States v. Schmidt, 373 F.3d 110, 101 (2d Cir. 2004)). The FBI learned that Brian Bass and his mother lived together, and Bass was a member of an e-group entitled "Candyman," and because of his membership to such a group, he probably possessed child pornography. Bass admitted viewing child pornography, but that he had never purposely saved or downloaded or copied any images to his computer. Bass and his mother

admitted that she found images that were deleted at her request. The police used two programs to recover images on the computer, ENCASE and SNAGIT. ENCASE recovered over 200 images of child pornography. SNAGIT recovered 39 images in the computer's unallocated space. Bass, at 1200. The officer also found a file in the unallocated space, which discussed how to remove information from the computer. Id. Bass is distinguished from Tucker, in that Bass claims that "he did not know the images were being automatically saved." Bass, at 1202. In answering the second unanswered question in Tucker, the Court held that the jury could reasonably infer that Bass knew child pornography was automatically saved to his mother's computer based on evidence that Bass attempted to remove the images. There was evidence that Bass used two programs, "History Kill," and "Window Washer," in an attempt to remove the child pornography. Id. The court concluded that there was sufficient evidence that the defendant knowingly possessed child pornography.

The Ninth Circuit also addressed the sufficiency of evidence to find the defendant guilty of possession of child pornography based upon the defendant's admitted "mere viewing of child pornography," United States v. Romm,455 F.3d 990, 997 (9th Cir. 2006). Romm challenged his conviction arguing that he merely viewed the images for about five minutes without downloading, saving or storing the images. Romm admits that he acted with the requisite mental state of "knowing," but he had no intent to possess the images. The Ninth Circuit disagreed, and held that,

> In the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control of it. (citing United States v. Tucker, 305 F.3d 1193 (10th Cir. 2002), citations omitted). Here, we hold Romm exercised dominion and control over the images in

> his cache by enlarging them on his screen, and saving them there for five minutes before deleting them. While the images were displayed on Romm's screen and simultaneously stored to his laptop's hard drive, he had the ability to copy, print, or email the images to others. Thus, this evidence of control was sufficient for the jury to find that Romm possessed and received the images in his cache.

Romm, at 997

The court also accepted the definition of possession as defined by BLACK'S LAW DICTIONARY 1183 (7th Ed. 1999), as "[t]he fact of having or holding property in one's power; the exercise of dominion over property." Further, that "the government must prove a sufficient connection between the defendant and the contraband to support the inference that the defendant exercised dominion and control over [it]." Tucker, at 1204.

In the instant case, Platt admitted that he had been involved in pornography on the Internet for a long time. Platt responded, "[n]ot very much child," when asked whether he was involved in adult and child pornography. Platt had not denied that the computer belonged to him. The large number of material found on the computer in the drive free space is a clear indicator of the defendant's intent, knowing desire to possess child pornography. For example, the government expects the evidence to prove that Platt's computer contained 1,827 images of suspected child pornography, 75 document/text files, 50 cartoon drawings, 488 images of child erotica, and 86 Web banners. The 86 Web banners describe sites that are clearly child pornography, for those individuals interested in child pornography. An example of such a site would be, "young porn," or "tiny-virgins."

The fact that these images are deleted, or when they were deleted, becomes irrelevant, since the defendant possessed the computer which contained the images.

Conclusion

Based upon the cases discussed above, the government submits that the defendant's challenge to the search of the deleted files contained on Platt's computer, which was in his possession, is meritless. The defendant has not denied that he possessed the computer. In fact, Cpl. Johnny Russell testified during the suppression hearing that the defendant told him that they did not need a search warrant to seize the computer, he would have given it to them. Further, the only issue that is challenged is what dates the images may have been deleted. Since the above case law is clear that the defendant had dominion and control over the computer and the images, the date of deletion does not change the fact that the defendant possessed child pornography.

Respectfully submitted on this 19th day of 2007.

LEURA G. CANARY
UNITED STATES ATTORNEY

s/Tommie Brown Hardwick
TOMMIE BROWN HARDWICK
One Court Square, Suite 201
Montgomery, AL 36104
Phone: (334) 223-7280
Fax: (334) 223-7135
E-mail: tommie.hardwick@usdoj.gov
ASB4152 W86T

IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE MIDDLE DISTRICT OF ALABAMA
NORTHERN DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	**CR. NO. 2:06cr214-MEF-WC**
	)	
DANIEL L. PLATT	)	

CERTIFICATE OF SERVICE

I hereby certify that on January 19, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following: Susan G. James, Esq.

Respectfully submitted,

s/Tommie Brown Hardwick
TOMMIE BROWN HARDWICK
One Court Square, Suite 201
Montgomery, AL 36104
Phone: (334)223-7280
Fax: (334)223-7135
E-mail: tommie.hardwick@usdoj.gov
ASB4152 W86T